Geofencing the Faithful: Smartphone Location Data, Foreign Influence Operations, and the Targeting of Religious Communities in the Digital Age

Douglas C. Youvan

doug@youvan.com www.youvan.ai

June 21, 2026

Smartphones have become persistent sensors of human movement, continuously reporting location through GPS, Wi-Fi, cellular networks, and embedded advertising software development kits. This infrastructure enables geofencing, a technique that draws virtual boundaries around real-world locations and triggers targeted content when devices enter or exit those zones. Once a device identifier is captured, it can be retargeted across apps, browsers, and platforms long after the individual has left the physical site. While originally developed for commercial marketing, geofencing has matured into a tool for precise behavioral influence. In 2025, public records revealed a U.S. firm registered under the Foreign Agents Registration Act proposed what it described as the largest Christian church geofencing campaign in U.S. history on behalf of a foreign government ministry. The plan targeted the physical boundaries of hundreds of evangelical and other Christian churches and colleges during worship and class times, with the intent to identify attendees' devices and deliver tailored digital messaging. This paper provides a technical explanation of how smartphones are captured by geofences, examines the 2025 case in detail, and analyzes its implications across technology, law, privacy, geopolitics, ethics, and religious community life. It situates the episode within broader patterns of surveillance capitalism and state-sponsored information operations, offering a framework for understanding how location data can convert ordinary movement into a vector for influence while raising urgent questions about consent, autonomy, and the protection of sacred spaces in an algorithmic era.

Keywords: geofencing, smartphone location data, foreign influence operations, targeted digital propaganda, FARA, evangelical churches, privacy surveillance, location-based advertising, Christian communities, information warfare, data brokers, digital enclosure, surveillance capitalism.

A collaboration with Grok 4.3 Expert. CC4.0.

https://orcid.org/0009-0004-4206-4253

Outline

1. The Technical Architecture of Smartphone Geofencing 1.1 Core Location Determination Technologies 1.2 Advertising SDKs, Device Identifiers, and Data Flows 1.3 Geofence Creation, Trigger Logic, and Persistent Retargeting 1.4 Accuracy, Scale, and Limitations of Current Systems

2. The Evolution from Commercial Marketing to Influence Operations 2.1 Historical Development of Location-Based Advertising 2.2 Integration with Political and Advocacy Campaigning 2.3 State and Proxy Actors Adopting Commercial Infrastructure 2.4 Distinguishing Legitimate Outreach from Coordinated Influence

3. The 2025 Case: Show Faith by Works and the Israeli Ministry of Foreign Affairs 3.1 Origins, Registration, and Contractual Framework under FARA 3.2 Stated Objectives and Messaging Strategy 3.3 Proposed Targeting Methodology and Geographic Scope 3.4 Complementary Elements: Exhibits, Content Creation, and Grassroots Plans 3.5 Public Disclosure, Media Coverage, and Initial Reactions

4. Legal and Regulatory Landscape 4.1 Foreign Agents Registration Act Requirements and Disclosure 4.2 Privacy Statutes, Data Broker Regulations, and Location Data 4.3 FTC Actions on Sensitive Location Data and Church Settings 4.4 Gaps in Current Oversight of Programmatic Advertising

5. Privacy, Consent, and the Sanctity of Religious Spaces 5.1 Erosion of Meaningful Consent in Pervasive Tracking Environments 5.2 Special Considerations for Places of Worship and Faith Communities 5.3 Psychological and Social Effects of Targeted Messaging in Sacred Contexts 5.4 Data Brokerage and the Commodification of Religious Attendance

6. Geopolitical Context and Information Warfare Dimensions 6.1 State Strategies for Shaping Foreign Public Opinion 6.2 The Role of Digital Influence in Broader Conflict Narratives 6.3 Comparisons with Other Documented Foreign and Domestic Operations 6.4 Transparency Mechanisms as Both Safeguard and Flashpoint

7. Impact on Evangelical and Broader Christian Communities 7.1 Theological and Ecclesial Responses to External Targeting 7.2 Effects on Trust, Autonomy, and Internal Discourse 7.3 Generational Differences in Reception of Digitally Delivered Messaging 7.4 Long-Term Implications for Church-State and Community Relations

8. Ethical Frameworks for Evaluating Location-Based Influence 8.1 Autonomy, Manipulation, and the Problem of Hidden Persuasion 8.2 Justifications Offered by Practitioners versus Critical Perspectives 8.3 Religious Ethics and the Protection of Sacred Gathering Spaces 8.4 Balancing Legitimate Advocacy with Coercive Potential

9. Comparative Cases and Pattern Recognition 9.1 Domestic Political Uses of Church and Event Geofencing 9.2 Corporate and Nonprofit Applications in Sensitive Locations 9.3 Emerging Examples Involving Other Faith Traditions or Ideological Groups 9.4 Lessons for Identifying and Analyzing Future Operations

10. Countermeasures, Resilience, and Policy Options 10.1 Individual and Community-Level Technical Protections 10.2 Platform, Browser, and Operating System Interventions 10.3 Regulatory and Legislative Proposals 10.4 Role of Religious Institutions in Setting Boundaries

11. Future Trajectories: AI, Advanced Surveillance, and Evolving Tactics 11.1 Integration of Artificial Intelligence with Location Targeting 11.2 Expansion to Wearables, Vehicles, and Ambient Sensors 11.3 Potential for More Sophisticated Narrative Delivery and Personalization 11.4 Anticipating Adaptive Responses by Targeted Communities

12. Conclusions and Recommendations 12.1 Synthesis of Technical, Legal, Ethical, and Social Findings 12.2 Recommendations for Policymakers, Platforms, and Faith Communities 12.3 Areas for Further Research and Interdisciplinary Inquiry

13. References

Art

1. The Technical Architecture of Smartphone Geofencing

Smartphone geofencing operates at the intersection of hardware sensors, operating system permissions, application software development kits, and large-scale advertising networks. The process begins when a device continuously or periodically determines its geographic position and shares that information with applications that have been granted location access. Once inside a predefined virtual boundary, the system can initiate actions ranging from immediate content delivery to the long-term association of the device with custom audience segments for subsequent messaging. This architecture relies on commercial infrastructure originally built for retail and marketing purposes but readily adaptable to more directed influence objectives. Understanding its components requires examining how location is established, how data moves through ecosystems of apps and platforms, how boundaries are enforced in practice, and what constraints shape the overall effectiveness and reach of such systems.

1.1 Core Location Determination Technologies

Modern smartphones determine position through multiple overlapping methods that trade off accuracy, power consumption, and availability. The primary outdoor technology remains the Global Positioning System, which uses signals from constellations of satellites to calculate latitude, longitude, and altitude with typical accuracies of a few meters under open-sky conditions. When satellite signals are weak or unavailable, devices supplement GPS with assisted GPS, which incorporates coarse positioning data from cellular networks and known Wi-Fi access points to accelerate fixes and improve reliability in urban canyons or indoors. Wi-Fi-based positioning works by matching the unique identifiers and signal strengths of nearby wireless networks against large databases of mapped locations, enabling positioning even when GPS is disabled or obstructed. Cellular triangulation estimates position by measuring signal timing or strength from multiple cell towers, providing lower-resolution but always-available coverage. Additional refinement comes from onboard sensors such as accelerometers, gyroscopes, and barometers, which enable dead-reckoning between fixes and floor-level altitude estimation in multi-story buildings. Bluetooth beacons placed in specific venues can further increase precision to sub-meter levels when devices are configured to scan for them. These technologies operate continuously in the background on most devices unless explicitly restricted by the user or operating system, creating a persistent stream of location signals that applications and embedded libraries can access.

1.2 Advertising SDKs, Device Identifiers, and Data Flows

The practical capture of location data at scale occurs primarily through advertising software development kits embedded in thousands of everyday applications. Developers integrate these libraries to monetize free or freemium apps by displaying targeted advertisements. Once an

application receives location permission from the user—often granted broadly as “allow all the time” for convenience—the SDK can periodically query the device’s current position and transmit it along with other signals to remote advertising servers. These transmissions typically include a persistent device-level identifier such as the Google Advertising ID on Android devices or the Identifier for Advertisers on iOS devices. Although both platforms now offer mechanisms for users to reset these identifiers or limit tracking, the identifiers remain stable enough over periods of days or weeks to support audience building. Data flows move from the individual device through the application to the ad network’s servers, where location coordinates are matched against active geofence definitions. Additional context such as app usage patterns, time of day, and inferred demographics may be combined to enrich the profile associated with the device identifier. Data brokers and aggregators further amplify reach by purchasing or licensing location histories from multiple sources and reselling access to marketers or other entities seeking to reach people who have visited particular categories of locations. The result is an ecosystem in which location information collected for one purpose can be repurposed across numerous downstream applications without the original user’s direct awareness of each recipient.

1.3 Geofence Creation, Trigger Logic, and Persistent Retargeting

Sponsors or their agencies create geofences by specifying geographic coordinates and boundaries through web-based dashboards or programmatic advertising platforms. Boundaries may take the form of simple circular radii centered on a point of interest or more complex polygons that follow the actual footprint of a building or campus. Time windows can be layered on top of spatial definitions so that triggers activate only during designated periods, such as worship services or class hours. Once defined, the geofence resides on the advertising platform’s servers. Detection occurs when any participating application on a device reports a location that falls inside the boundary; the platform then evaluates whether the device identifier matches criteria for immediate action or audience inclusion. Immediate actions may include serving a banner advertisement, video placement, or push notification within apps that have integrated the relevant SDK. More commonly, the system records the device identifier in a custom audience list. This list subsequently enables retargeting: the same device can receive related messaging across unrelated apps, mobile websites, and even connected television environments long after it has left the original location. Retargeting lists persist according to platform policies, often for weeks or months, and can be refreshed whenever the device re-enters the geofence or exhibits related behavioral signals. The architecture therefore separates the moment of physical presence from the moment of message delivery, allowing sustained influence campaigns built on a single visit to a target site.

1.4 Accuracy, Scale, and Limitations of Current Systems

Geofencing achieves sufficient precision for many influence objectives because GPS routinely delivers meter-level accuracy outdoors and Wi-Fi or beacon augmentation improves performance in dense environments. In practice, platforms often accept coarser location signals for broader reach while reserving high-precision triggers for campaigns that justify the narrower audience. Scale derives from the enormous installed base of smartphones and the density of applications containing advertising libraries; even modest permission rates across popular apps produce coverage of large populations. Real-time bidding systems evaluate millions of ad impressions per second, enabling rapid matching of devices to active geofences. Nevertheless, several constraints limit universal effectiveness. Operating system updates have introduced more granular permission controls, requirements for user consent dialogs, and options for approximate rather than precise location sharing. On iOS, the App Tracking Transparency framework requires explicit opt-in for cross-app tracking that supports many retargeting use cases. Battery optimization features can throttle background location updates. Users who regularly reset advertising identifiers or employ privacy-focused browsers and virtual private networks reduce the persistence of device-level tracking. Regulatory scrutiny of data brokers selling location data derived from sensitive venues has also prompted some platforms to restrict certain categories of geofencing. Despite these limitations, the underlying sensor and network infrastructure continues to support robust location-aware advertising at population scale, and incremental improvements in 5G positioning and sensor fusion are likely to increase both accuracy and indoor reliability in coming years.

2. The Evolution from Commercial Marketing to Influence Operations

The technical capabilities described in the preceding section were not developed for geopolitical or ideological purposes. They emerged from the commercial imperative to connect advertisers with potential customers at moments of high intent. Over time, however, the same sensor infrastructure, data flows, and audience-building mechanisms proved equally serviceable for political persuasion, advocacy, and eventually state-directed influence campaigns. This evolution did not require the invention of new technologies so much as the creative repurposing of existing ones by actors with different objectives and different levels of resources. Understanding how geofencing moved from retail promotions to targeted messaging inside places of worship illuminates both the flexibility of the underlying systems and the shifting boundaries between ordinary marketing and more consequential forms of behavioral influence.

2.1 Historical Development of Location-Based Advertising

Location-based advertising began with relatively simple proximity marketing. Retailers and service providers defined virtual boundaries around their own stores or the stores of competitors and arranged for mobile advertisements or offers to appear when a device entered those zones. Early implementations relied on basic GPS coordinates and circular radii, often delivered through dedicated applications or short message service. As smartphone penetration increased and advertising networks matured, the practice expanded to include programmatic platforms capable of real-time bidding across thousands of applications. Data brokers entered the ecosystem by aggregating location histories from multiple sources and offering segments such as “people who visited a particular category of venue within the last thirty days.” This aggregation allowed advertisers to reach audiences even when those individuals were no longer physically present at the original site. The business model proved highly effective for driving foot traffic, measuring campaign lift through location verification, and building persistent customer profiles. Because the infrastructure was already paid for by commercial demand, the marginal cost of extending its use to non-commercial objectives remained low.

2.2 Integration with Political and Advocacy Campaigning

Political consultants and advocacy organizations recognized that the same location signals could identify individuals at politically relevant sites. Campaigns began defining geofences around polling places, rallies, competitor events, and, in some documented instances, houses of worship. One early and widely noted domestic example involved efforts to reach Catholic voters attending Sunday Mass by placing virtual boundaries around church properties and serving advertisements during or immediately after services. The logic was straightforward: presence at a religious service could serve as a proxy for certain values or demographic characteristics, allowing messages tailored to those inferred characteristics to be delivered with high temporal and spatial relevance. Advocacy groups on multiple sides of contested issues adopted similar tactics, using attendance at rallies, protests, or community meetings as triggers for follow-up digital contact. These applications remained within the commercial advertising ecosystem; campaigns purchased impressions through the same demand-side platforms used by retailers. The primary innovation lay in the choice of target locations and the framing of messages rather than in any alteration of the underlying data pipelines.

2.3 State and Proxy Actors Adopting Commercial Infrastructure

Foreign governments and their authorized representatives began to treat the same commercial infrastructure as a legitimate channel for public diplomacy and strategic communication. Because the advertising networks and data brokers operate globally and accept clients through standard business relationships, a state actor could, in principle, define geofences around

locations where desired audiences congregate and purchase targeted impressions without building dedicated surveillance systems. In practice, such efforts are often routed through domestic intermediaries required to register under foreign agent disclosure statutes. These intermediaries translate strategic objectives into campaign parameters—selecting locations, defining time windows, crafting creative content, and managing audience lists—while the actual delivery occurs through the same real-time bidding exchanges that serve ordinary commercial advertisements. The 2025 proposal to geofence hundreds of Christian churches and colleges across multiple U.S. states illustrates this pattern. A newly formed entity registered under the Foreign Agents Registration Act outlined plans to use existing location-based advertising tools to identify devices present during worship services and to deliver messaging intended to shape attitudes toward a foreign government's policies. The technical execution relied entirely on commercial geofencing capabilities; the novelty resided in the scale, the choice of sensitive venues, and the explicit foreign governmental sponsorship disclosed through regulatory filings.

2.4 Distinguishing Legitimate Outreach from Coordinated Influence

The boundary between ordinary advocacy and coordinated foreign influence is not always sharp in technical terms, because the delivery mechanisms are identical. Distinctions therefore rest on questions of sponsorship, transparency, intent, and the nature of the venues being targeted. Domestic political campaigns operate under election laws and disclosure requirements that differ from those governing foreign agents. Religious institutions may view external messaging delivered inside or immediately adjacent to their properties as an intrusion on sacred space regardless of the sponsor's identity. When a foreign principal funds a campaign that systematically maps places of worship and seeks to capture the devices of attendees for retargeting, the activity raises additional questions about the appropriate limits of public diplomacy in democratic societies. Transparency mechanisms such as foreign agent registration provide one layer of visibility, yet they do not prevent the underlying data capture or message delivery. Communities and individuals must therefore rely on a combination of technical self-protection, platform policies, and regulatory oversight to maintain meaningful control over when and how their physical presence at particular locations becomes the basis for targeted digital persuasion. The evolution from retail promotions to state-sponsored geofencing of religious gatherings demonstrates how quickly commercial tools can be adapted to new strategic purposes once the technical and economic barriers to entry have been lowered.

3. The 2025 Case: Show Faith by Works and the Israeli Ministry of Foreign Affairs

In September 2025 a newly formed California-based entity filed documents with the U.S. Department of Justice disclosing its role as a foreign agent acting on behalf of the Israeli

Ministry of Foreign Affairs. The filing described an ambitious outreach program that included what the registrants characterized as the largest Christian church geofencing campaign in U.S. history. The proposed effort centered on mapping the physical boundaries of hundreds of churches and Christian colleges across several western states and using location data to identify devices present during worship services or class periods. Once captured, those devices would receive targeted digital messaging and be added to retargeting audiences for continued contact. Although the geofencing component later faced public criticism and was reportedly set aside in favor of other tactics, the original proposal provides a detailed window into how commercial geofencing infrastructure can be adapted for state-sponsored influence objectives directed at religious communities. The case illustrates both the technical feasibility of such operations and the regulatory, ethical, and communal questions they raise when sacred spaces become nodes in digital targeting networks.

3.1 Origins, Registration, and Contractual Framework under FARA

Show Faith by Works, LLC was incorporated in California in 2025 as a self-described Christian-based marketing and communications firm. Its principal, Chad Schnitger, registered the entity under the Foreign Agents Registration Act as an agent of the Israeli Ministry of Foreign Affairs. The registration disclosed an agreement valued in the range of several million dollars for activities that included public diplomacy and outreach to Christian audiences in the western United States. Funding was routed in part through established advertising intermediaries. The filing contained both a registration statement and an extensive exhibit that functioned as a campaign proposal or pitch deck. This exhibit outlined multiple lines of activity, one of which was the large-scale geofencing operation. The document listed specific churches by name and approximate attendance size, along with Christian colleges, and proposed time-bound geofencing during periods when worshippers or students would be present. The choice to register under FARA reflected the legal requirement that persons acting as agents of foreign principals in political or public relations activities disclose their relationship and activities to the Department of Justice.

3.2 Stated Objectives and Messaging Strategy

According to the materials submitted with the FARA filing, the overarching purpose of the campaign was to strengthen support for Israel among American Christians, particularly evangelicals, at a time when polling indicated declining approval in some demographic segments. The proposed messaging emphasized historical and biblical connections between Christians and the Jewish people, Israel's role as an ally, and security concerns framed around groups such as Hamas. The materials described plans to counter what the registrants characterized as low evangelical approval of Israel and to increase awareness of Palestinian ties to designated terrorist organizations. Content themes included portrayals of the October 7

attacks, historical narratives about the region, and arguments against certain political positions associated with Palestinian leadership. The messaging was intended to be delivered through multiple channels, with geofencing positioned as a high-precision method for reaching individuals already gathered in faith-based settings where receptivity to religiously framed arguments might be elevated. The proposal also referenced invitations for church groups to visit Israel and participation in related educational or experiential programs.

3.3 Proposed Targeting Methodology and Geographic Scope

The geofencing component called for drawing virtual boundaries around the actual footprints of major churches in California, Arizona, Nevada, and Colorado, with additional references to other states in supporting materials. Christian colleges were to be included on weekdays. Geofences were to be active primarily during worship times on Sundays and during scheduled class periods. The plan envisioned capturing device identifiers of individuals whose phones reported locations inside these boundaries through any participating application. Once identified, devices would be added to custom audiences for immediate or follow-up digital advertising across the broader mobile ecosystem. The filing included lists of specific congregations with estimated attendance figures, indicating a data-driven approach to prioritizing larger or strategically significant sites. The methodology relied entirely on existing commercial location-based advertising platforms rather than custom surveillance technology. Time restrictions were intended to align message delivery with moments when target audiences were physically assembled in the chosen venues, thereby increasing contextual relevance.

3.4 Complementary Elements: Exhibits, Content Creation, and Grassroots Plans

Beyond geofencing, the proposal outlined several parallel activities. One prominent element was a mobile exhibit described as an “October 7 Experience,” featuring a custom-built trailer with immersive displays, video content, and interactive components intended for deployment at churches, colleges, and Christian events. Additional plans involved the production of pastoral resource packages, short videos and podcasts featuring clergy or influencers, and efforts to recruit or compensate pastors and content creators for generating Israel-related materials. The filing also referenced search engine optimization and website development aimed at directing traffic toward favorable narratives. These elements were presented as mutually reinforcing: geofencing would identify and initially engage audiences, while experiential exhibits and content would deepen exposure and encourage further actions such as travel to Israel or participation in related programs. The overall structure combined high-tech targeting with traditional grassroots and experiential outreach methods.

3.5 Public Disclosure, Media Coverage, and Initial Reactions

Because the materials were filed under FARA, they became part of the public record and were subsequently reported by multiple news organizations. Coverage highlighted the scale of the proposed geofencing effort, the choice of religious venues as targeting locations, and the involvement of a foreign government ministry. Some churches listed in the documents stated they had not been contacted in advance and expressed surprise or concern about the use of their properties as geofence boundaries. Privacy advocates described the approach as invasive when applied to sensitive locations such as places of worship. In subsequent statements, the principal of Show Faith by Works indicated that the geofencing element had been reconsidered in light of public reaction and that the organization had shifted emphasis toward grassroots and educational activities. Updated FARA filings were anticipated to reflect the revised scope. The episode generated discussion within Christian communities about external influence in church settings, the ethics of location-based messaging, and the appropriate boundaries between public diplomacy and domestic religious life. The case remains notable as one of the most detailed public records of a foreign principal's use of commercial geofencing infrastructure directed at U.S. religious institutions.

4. Legal and Regulatory Landscape

The deployment of geofencing technology for targeted messaging occurs within a patchwork of disclosure requirements, privacy protections, and advertising industry practices rather than under a single comprehensive statute. When such capabilities are applied to sensitive locations such as places of worship, existing legal frameworks provide partial transparency and limited safeguards but leave significant gaps in oversight. The 2025 proposal to geofence churches and Christian colleges illustrated both the operation of these frameworks and their limitations. Foreign agent registration rules compelled public disclosure of the sponsorship and broad outlines of the planned activity, yet they did not prohibit the use of commercial location-based advertising tools or impose substantive restrictions on the choice of target venues. Privacy regulations address certain data practices but have not kept pace with the scale and precision of programmatic geofencing. This section examines the principal legal and regulatory structures that bear on such operations and identifies areas where current rules provide incomplete protection for individuals and communities.

4.1 Foreign Agents Registration Act Requirements and Disclosure

The Foreign Agents Registration Act establishes a disclosure regime for persons or entities acting as agents of foreign principals in political, public relations, or related activities within the United States. Registration requires submission of detailed information about the relationship with the

foreign principal, the nature of the activities undertaken, and the sources and amounts of funding involved. The statute aims to ensure that the American public and government officials are aware when foreign governments or their representatives seek to influence domestic opinion or policy. In the 2025 case, the filing by Show Faith by Works, LLC provided public notice of the contractual relationship with the Israeli Ministry of Foreign Affairs, the approximate value of the engagement, and the intended scope of outreach activities, including the geofencing component. The exhibit attached to the registration contained extensive detail on proposed targeting locations and messaging themes. While the disclosure mechanism functioned as designed by surfacing the existence and general parameters of the campaign, it did not trigger any automatic review or restriction on the content of the proposed activities. FARA remains primarily a transparency statute rather than a substantive regulatory barrier, leaving the actual execution of disclosed plans subject to other legal constraints or public reaction.

4.2 Privacy Statutes, Data Broker Regulations, and Location Data

United States privacy law is sectoral rather than comprehensive at the federal level, with significant variation across states. California's privacy statutes, relevant because the registering entity was based in that state, grant consumers rights to know what personal information is collected about them, to request deletion, and to opt out of the sale or sharing of their data. Location data is explicitly included within the scope of protected personal information under these laws. However, enforcement in the context of programmatic advertising remains challenging because location signals are often collected and processed through complex chains of applications, software development kits, and data brokers before reaching the entity that ultimately defines a geofence. Data brokers that aggregate and sell location histories derived from mobile devices have faced increasing regulatory attention, particularly when the data pertains to sensitive venues. Even where consumers possess formal rights, exercising them effectively against the diffuse ecosystem of ad networks and brokers is difficult. The result is that individuals whose devices are captured by a geofence around a church may have limited practical ability to prevent or retroactively control the use of that location signal for targeted messaging.

4.3 FTC Actions on Sensitive Location Data and Church Settings

The Federal Trade Commission has taken enforcement actions against data brokers for practices involving the collection and sale of location data from sensitive locations, including places of worship, medical facilities, and other venues where individuals may have heightened expectations of privacy. These actions have emphasized that the sale of precise location data without adequate safeguards or consumer consent can constitute unfair or deceptive practices. In principle, such enforcement provides a deterrent against the most egregious forms of location data commercialization. Nevertheless, the actions have focused primarily on the

conduct of data brokers rather than on the downstream use of location data by advertisers or foreign agents who purchase access through standard advertising platforms. There is no specific federal prohibition on geofencing religious institutions for messaging purposes, nor are there mandatory review processes for campaigns that target such venues. The absence of tailored rules for sensitive locations means that commercial geofencing tools can be applied to churches or similar sites in the same manner as they are applied to retail stores or event venues, provided the technical and contractual arrangements with advertising networks are in place.

4.4 Gaps in Current Oversight of Programmatic Advertising

Programmatic advertising operates through real-time bidding systems that match advertisers with available impressions across vast numbers of applications and websites. These systems are governed largely by industry self-regulation and platform policies rather than detailed statutory requirements specific to geofencing or location-based influence. Platforms maintain terms of service that prohibit certain categories of content or targeting, yet enforcement is inconsistent and often reactive. There is no dedicated regulatory body charged with reviewing geofencing campaigns for potential harm to religious communities or other sensitive groups. When a foreign principal uses a registered domestic agent to conduct such a campaign, the primary legal obligation remains disclosure under FARA rather than prior approval or substantive restrictions on venue selection. This structure creates a regulatory environment in which technically sophisticated location-based operations can be planned and, in some cases, executed with relatively limited ex ante oversight. The gaps are particularly noticeable when the targeting relies on the existing commercial infrastructure rather than on bespoke surveillance tools, because the activity can be characterized as ordinary advertising even when its sponsor and objectives are geopolitical. Closing these gaps would require either expanded substantive regulation of location-based advertising or stronger norms within religious and civic institutions regarding the acceptable boundaries of external digital engagement.

5. Privacy, Consent, and the Sanctity of Religious Spaces

The application of geofencing technology to places of worship raises distinct questions that extend beyond general concerns about location tracking. Religious gatherings are settings in which individuals often expect a measure of seclusion from commercial and political surveillance, and in which participation carries communal and spiritual significance. When devices are identified and messaging is triggered by presence at these locations, the boundary between public space and protected gathering is blurred. The 2025 proposal to geofence churches and Christian colleges made these tensions concrete by treating attendance at worship services as a reliable signal for targeted digital influence. This section examines how pervasive

tracking environments undermine traditional notions of consent, why religious venues warrant special consideration, and how the commodification of location data transforms participation in faith communities into a marketable attribute.

5.1 Erosion of Meaningful Consent in Pervasive Tracking Environments

Consent to location data collection is typically obtained through application permission prompts that users encounter when installing or updating software. These prompts are often framed in broad terms that emphasize functionality such as navigation or personalized recommendations rather than the downstream uses of the data in advertising ecosystems or influence campaigns. Once granted, location permission frequently remains active in the background, allowing continuous or frequent reporting even when the user is not actively engaging with the application. The resulting data flows into complex networks of software development kits, advertising exchanges, and data brokers where individual control becomes impractical. Users may understand that their phone knows where they are, yet they rarely possess a clear picture of how that information is aggregated, sold, or used to construct persistent profiles that follow them across contexts. In this environment, the initial grant of permission functions more as a one-time procedural step than as ongoing, informed consent to every subsequent use of the location signal. When a geofence around a church captures a device and adds it to a retargeting audience, the individual has not provided specific authorization for messaging linked to their religious attendance.

5.2 Special Considerations for Places of Worship and Faith Communities

Places of worship occupy a distinctive position in social and legal thought. They are spaces where individuals gather for reasons that are simultaneously personal, communal, and often transcendent. Historical and constitutional traditions in many societies have afforded religious exercise a degree of protection from undue state or commercial intrusion. Geofencing these locations converts a spiritual or communal act into a detectable behavioral signal that can be monetized or weaponized for external messaging. The 2025 filing proposed to treat the physical boundaries of churches as reliable indicators of receptive audiences for content aligned with a foreign government's strategic communications goals. This approach assumes that presence during worship reliably correlates with particular beliefs or openness to certain narratives. Such an assumption risks reducing complex religious participation to a data point while disregarding the diversity of views that may exist within any single congregation. Faith communities may therefore experience geofencing not merely as another form of advertising but as an external claim on the attention and loyalty of their members at the very moment those members are engaged in collective religious practice.

5.3 Psychological and Social Effects of Targeted Messaging in Sacred Contexts

When individuals receive digital messages that appear to follow them from a worship service into their broader online experience, the psychological impact can extend beyond simple irritation at unwanted advertising. The sensation that one's religious attendance has been observed and acted upon by distant actors may erode the sense of sanctuary that many associate with places of worship. Members of targeted communities may begin to question whether their presence at services is truly private or whether it has become visible to commercial and political networks. This awareness can introduce self-consciousness into what was previously an unmonitored space, altering the quality of communal participation. Socially, the practice can strain relationships between congregants and church leadership if members perceive that their institution has been mapped and exploited without prior consultation. In the 2025 case, several listed congregations reported that they had not been contacted before their properties appeared in the targeting materials, amplifying perceptions of external overreach. Over time, repeated exposure to contextually linked messaging may also shape how individuals interpret their own religious commitments, either reinforcing or undermining particular theological or political alignments depending on the content delivered.

5.4 Data Brokerage and the Commodification of Religious Attendance

Data brokers occupy a central position in the infrastructure that makes large-scale geofencing feasible. By purchasing and combining location signals from numerous applications, these entities construct detailed movement profiles that can be segmented according to visited locations. Attendance at a church or religious college can become one attribute among many in a marketable profile, allowing purchasers to reach individuals who frequent such venues even if they never installed a specific application associated with the targeting campaign. This commodification transforms religious participation from a protected communal activity into a commercially valuable signal. The economic incentive to collect and sell such data persists regardless of the downstream use, whether that use is retail promotion or geopolitical messaging. In the context of the 2025 proposal, the ability to identify devices inside church boundaries depended on the prior aggregation of location data by brokers and ad networks. The resulting system creates a structural asymmetry: individuals contribute location information through ordinary app usage, while organized actors with sufficient resources can query that information to reach them at moments of religious gathering. This dynamic raises fundamental questions about whether the current architecture of location data markets adequately accounts for the special status of religious and other sensitive venues.

6. Geopolitical Context and Information Warfare Dimensions

States have long sought to shape opinion in foreign societies through public diplomacy, cultural programs, and media outreach. Digital technologies have accelerated and refined these efforts by enabling precise, scalable, and often covert forms of messaging. Geofencing represents one node in this larger ecosystem of information operations, allowing actors to link physical presence at specific sites with targeted digital content. The 2025 proposal to geofence Christian churches and colleges in the United States fits within a pattern of state actors leveraging commercial advertising infrastructure to pursue strategic communication objectives abroad. This section situates such operations within evolving state strategies for influencing foreign publics, examines their integration into broader conflict narratives, compares them with other documented efforts, and assesses the dual role of transparency mechanisms in both enabling oversight and generating friction.

6.1 State Strategies for Shaping Foreign Public Opinion

Governments routinely allocate resources to influence how populations in other countries perceive their policies, values, and security interests. Traditional instruments have included state-supported broadcasting, cultural exchanges, and support for sympathetic organizations. Contemporary strategies increasingly incorporate digital platforms because they offer low marginal cost, high reach, and the capacity for micro-targeting based on behavioral signals. Location data adds a layer of contextual precision by allowing messages to be delivered when individuals are physically present in environments presumed to correlate with particular worldviews or openness to certain arguments. In the 2025 case, the decision to focus geofencing on churches during worship times reflected an assumption that religious settings could serve as high-value nodes for reaching audiences receptive to religiously framed messaging about international affairs. This approach aligns with broader patterns in which states identify demographic or institutional gateways—such as faith communities, universities, or diaspora networks—and seek to amplify favorable narratives within them. The use of registered domestic intermediaries further allows foreign principals to operate within the legal and commercial structures of the target society while maintaining strategic direction from abroad.

6.2 The Role of Digital Influence in Broader Conflict Narratives

Information operations have become integral to contemporary conflicts, often described by practitioners as additional fronts alongside kinetic and economic dimensions. Digital influence campaigns aim to shape the information environment in ways that support or undermine political will, alliance cohesion, and public legitimacy. Geofencing contributes to this environment by converting everyday movement into opportunities for narrative insertion.

When a device is identified inside a church and subsequently receives content linking religious identity to specific foreign policy positions, the operation blurs the boundary between spiritual life and geopolitical contestation. In the materials associated with the 2025 filing, messaging themes explicitly connected biblical interpretation, historical claims, and contemporary security concerns. Such efforts participate in larger struggles over how conflicts are framed for external audiences, particularly in societies where religious communities hold significant cultural and political influence. The precision offered by location-based targeting allows these narratives to be delivered with temporal and spatial relevance that traditional media cannot easily replicate, potentially increasing their perceived authenticity or urgency among recipients.

6.3 Comparisons with Other Documented Foreign and Domestic Operations

The 2025 church geofencing proposal shares structural features with both domestic political uses of location targeting and other foreign influence efforts. Within the United States, political campaigns and advocacy groups have employed geofencing around polling sites, rallies, and houses of worship to reach voters or supporters with contextually relevant messages. These domestic applications operate under election and lobbying disclosure rules that differ from foreign agent requirements. Internationally, multiple states have been documented using social media manipulation, state-linked media outlets, and advertising networks to advance narratives in target countries. The distinctive element in the church geofencing case lies in the systematic mapping of religious institutions as primary targeting vectors and the explicit linkage of physical attendance at worship with device-level retargeting. While many influence operations focus on online communities or broad demographic segments, this approach treated the physical architecture of faith communities as a reliable proxy for audience segmentation. The subsequent public disclosure and partial retrenchment of the geofencing component also illustrate how transparency requirements can alter the trajectory of such operations once they enter the public domain.

6.4 Transparency Mechanisms as Both Safeguard and Flashpoint

Foreign agent registration statutes serve as primary transparency tools for monitoring external influence activities. By requiring disclosure of relationships, funding, and intended activities, these mechanisms enable public scrutiny and governmental awareness. In the 2025 instance, the filing process brought the proposed geofencing campaign into view, prompting media examination, statements from affected churches, and commentary from privacy advocates. This visibility functioned as a safeguard by surfacing the operation before full implementation and contributing to the decision to de-emphasize the geofencing element. At the same time, disclosure requirements can become flashpoints when the revealed activities involve sensitive domestic institutions such as religious congregations. Affected communities may perceive the targeting itself as an infringement, while the disclosing party may view registration as sufficient

compliance that does not preclude the underlying strategy. The dual character of transparency mechanisms therefore creates ongoing tension between the benefits of public knowledge and the potential for disclosed plans to generate backlash that complicates the very influence objectives they were meant to advance. Effective governance of location-based influence operations will likely require both robust disclosure rules and clearer normative boundaries around the use of commercial tracking tools in religious and other protected settings.

7. Impact on Evangelical and Broader Christian Communities

The proposal to geofence churches and Christian colleges in 2025 directly implicated communities whose members gather for worship, study, and fellowship. For many participants, these settings represent spaces of spiritual refuge and collective identity rather than sites for external political or commercial engagement. When location data from these gatherings becomes the basis for targeted digital messaging, the effects extend beyond individual device users to the social fabric of congregations and the broader evangelical landscape. This section examines how such operations intersect with theological self-understanding, internal trust dynamics, generational differences in media reception, and longer-term relationships between faith communities and external actors.

7.1 Theological and Ecclesial Responses to External Targeting

Christian communities have historically navigated tensions between engagement with the wider world and the preservation of distinct spiritual identity. The idea that devices carried into worship services could be identified and subsequently used to deliver messages aligned with foreign policy objectives raises questions about the boundaries of the church as a distinct sphere. Some theological perspectives emphasize the church's calling to engage public issues and discern truth in all domains, potentially viewing external content as one input among many for critical reflection. Other perspectives stress the sanctity of gathered worship and the importance of protecting communal spaces from instrumentalization by political or commercial interests. In the 2025 case, several congregations listed in the targeting materials expressed surprise that their properties had been mapped without prior consultation, framing the episode as an external claim on their communal life. Ecclesial responses have included calls for greater awareness of digital surveillance practices and discussion of how churches might establish clearer boundaries regarding external digital outreach conducted on or near their premises.

7.2 Effects on Trust, Autonomy, and Internal Discourse

The knowledge that one's presence at a worship service could trigger targeted messaging can introduce a subtle but persistent awareness of external observation into what many experience as a protected gathering. This awareness may affect the quality of participation, as individuals

weigh whether their attendance contributes to data profiles used for purposes outside their control. Within congregations, the episode can generate discussion about institutional autonomy and the extent to which church leadership should proactively address digital targeting of members. Trust dynamics may shift if congregants perceive that their institution has been rendered visible to outside actors without sufficient safeguards or communication. Internal discourse may also become polarized, with some members viewing the proposed outreach as legitimate advocacy or education while others see it as an unwelcome intrusion that compromises the church's independence. These tensions are amplified when the targeting is linked to a foreign principal, raising additional questions about the appropriate relationship between domestic religious communities and international geopolitical actors.

7.3 Generational Differences in Reception of Digitally Delivered Messaging

Evangelical communities are not monolithic in their relationship to digital media or in their views on international issues. Younger generations, having grown up with pervasive smartphone use and algorithmic content delivery, may exhibit greater familiarity with targeted advertising yet also heightened sensitivity to privacy concerns and perceived manipulation. Older generations may place higher value on traditional forms of religious authority and community cohesion while expressing varying degrees of openness to digital engagement. In the context of messaging about Israel and related Middle East issues, polling has indicated notable generational divergence in levels of support and in the theological frameworks used to interpret contemporary events. Digitally delivered content that follows individuals from worship settings may therefore encounter different reception patterns across age cohorts. Younger participants, already navigating competing online narratives, may subject such messages to greater scrutiny or integrate them into existing skepticism toward institutional sources. Older participants may experience the same messages as extensions of familiar advocacy efforts or as novel intrusions into established patterns of religious life.

7.4 Long-Term Implications for Church-State and Community Relations

Sustained use of location-based targeting directed at religious institutions could contribute to longer-term shifts in how faith communities understand their relationship to both domestic authorities and foreign actors. If churches come to be routinely treated as nodes in digital influence networks, leaders may invest greater resources in digital literacy, data protection practices, and internal policies governing external engagement. At the societal level, the episode highlights tensions between the commercial availability of location data and the special status historically accorded to religious exercise. Communities may increasingly advocate for stronger norms or regulations that limit the use of precise location signals from places of worship for messaging purposes. Over time, these dynamics could influence broader conversations about the role of religious institutions in democratic societies and the extent to

which their physical gatherings should remain relatively insulated from systematic external observation and targeted influence. The 2025 case, even in its partially revised form, has already prompted some congregations and denominational bodies to address these questions more explicitly than before.

8. Ethical Frameworks for Evaluating Location-Based Influence

The use of geofencing to deliver targeted messages to individuals present at places of worship invites sustained ethical reflection. Such operations sit at the intersection of technological capability, commercial infrastructure, and strategic intent, raising questions about human autonomy, the nature of persuasion, and the appropriate limits of influence within sensitive social and spiritual contexts. The 2025 proposal to geofence churches and Christian colleges brought these issues into sharp relief by treating attendance at worship as a trigger for externally directed digital content. This section applies several ethical lenses to location-based influence, considering questions of autonomy and hidden persuasion, contrasting justifications offered by practitioners with critical perspectives, examining religious ethical traditions, and exploring the tension between legitimate advocacy and coercive potential.

8.1 Autonomy, Manipulation, and the Problem of Hidden Persuasion

Human autonomy is centrally concerned with the capacity of individuals to direct their own lives according to reasons and values they can reflectively endorse. When location data collected through everyday smartphone use is repurposed to deliver messages linked to a specific physical context—such as presence during worship—the individual may experience influence without having explicitly authorized that particular application of their data. The persuasion is hidden in the sense that the connection between the geofence trigger and the subsequent messaging is not transparent to the recipient at the moment of delivery. This opacity can undermine the conditions for autonomous response, as individuals may adjust their behavior or beliefs without full awareness of the mechanisms shaping the information environment they encounter. In the context of religious gatherings, the issue is compounded because participation often carries meanings that extend beyond consumer choice or political preference. When external actors systematically map and target these gatherings, the resulting influence operates on a domain that many participants regard as protected from instrumental external claims.

8.2 Justifications Offered by Practitioners versus Critical Perspectives

Practitioners of location-based outreach frequently frame their activities in terms of public diplomacy, education, or standard marketing practice. They emphasize that geofencing relies on existing commercial advertising systems rather than covert surveillance, that disclosure

requirements such as foreign agent registration provide transparency, and that individuals retain the ability to ignore or opt out of messages. From this perspective, the activity represents a legitimate effort to communicate with audiences presumed to hold relevant interests or values. Critical perspectives, by contrast, argue that the systematic targeting of religious venues introduces asymmetries of power and information that ordinary commercial advertising does not. They point to the special status of sacred spaces, the potential for foreign principals to shape domestic religious discourse, and the difficulty individuals face in understanding or controlling how their location signals are aggregated and deployed. The debate therefore turns less on the technical legality of the methods and more on whether the choice of target locations and the nature of the sponsor create distinctive ethical concerns that standard marketing ethics do not fully address.

8.3 Religious Ethics and the Protection of Sacred Gathering Spaces

Religious ethical traditions offer additional resources for evaluating location-based influence directed at faith communities. Many traditions emphasize the sanctity of gathered worship and the importance of protecting communal spaces from external domination or manipulation. Concepts such as stewardship of the community, the integrity of worship, and the responsibility to exercise discernment regarding outside influences provide normative frameworks for assessing whether geofencing churches constitutes an appropriate form of engagement or an unwarranted intrusion. From this vantage point, the ethical question is not solely whether individuals consent to data collection in general, but whether the church as a body has obligations to safeguard the conditions under which its members gather. The 2025 proposal, by treating church properties as high-value targeting sites without prior engagement with the institutions themselves, raised concerns that external actors were claiming a form of access to communal life that bypassed ordinary ecclesial processes of discernment and hospitality.

8.4 Balancing Legitimate Advocacy with Coercive Potential

A central ethical challenge lies in distinguishing legitimate forms of advocacy and public diplomacy from practices that cross into coercion or undue influence. Location-based targeting gains persuasive power precisely because it links messaging to the physical context of the recipient's activity. When that context is religious worship, the linkage can create an appearance of contextual endorsement that the recipient did not authorize. At the same time, religious communities have long engaged in public witness and have welcomed external perspectives on matters of shared concern. The ethical task is therefore to identify criteria that preserve space for genuine dialogue while protecting against systematic efforts to convert participation in worship into a reliable trigger for externally controlled messaging. Such criteria might include requirements for prior consultation with affected institutions, greater transparency about targeting logic, and stronger individual and collective controls over the use of location data

derived from sensitive venues. Without such safeguards, the technical capacity for precise geofencing risks outpacing the ethical and institutional norms needed to govern its application in domains where autonomy and communal integrity carry particular weight.

9. Comparative Cases and Pattern Recognition

The 2025 proposal to geofence Christian churches and colleges did not emerge in isolation. It represents one instance within a broader pattern of actors using commercial location-based advertising infrastructure to identify and message individuals at specific physical sites. Similar techniques have been applied in domestic political campaigns, corporate marketing, nonprofit advocacy, and efforts targeting other faith traditions or ideological gatherings. Examining these cases reveals recurring patterns in how geofencing is operationalized, the types of locations selected, and the justifications offered by practitioners. This section surveys comparative examples across domestic political, corporate, and cross-faith contexts, then distills lessons for recognizing and analyzing future operations that employ location data as a vector for influence.

9.1 Domestic Political Uses of Church and Event Geofencing

Political campaigns and advocacy organizations within the United States have employed geofencing around houses of worship and political events to reach voters or supporters with contextually relevant messages. One documented approach involved placing virtual boundaries around Catholic parishes during Sunday services to deliver advertisements aligned with particular policy positions or candidate preferences. The underlying assumption was that attendance at religious services could serve as a behavioral proxy for values or demographic characteristics relevant to electoral mobilization. These domestic applications typically operate through standard programmatic advertising platforms and are subject to election-related disclosure rules rather than foreign agent requirements. The technical execution mirrors the 2025 church geofencing proposal in its reliance on device identifiers captured during specific time windows at designated locations. The primary differences lie in the domestic sponsorship and the explicit electoral framing, yet the core mechanism—converting presence at a faith gathering into a trigger for targeted digital content—remains consistent.

9.2 Corporate and Nonprofit Applications in Sensitive Locations

Corporations and nonprofit organizations have applied geofencing to a wide range of venues, including hospitals, schools, protest sites, and community centers. Retailers have used geofences around competitor locations to deliver promotional offers, while advocacy groups have targeted areas near legislative buildings or demonstration sites to mobilize supporters or counter opposing messages. In sensitive locations such as medical facilities or educational institutions, location-based targeting has raised concerns analogous to those surrounding

religious venues, particularly when the data is used to infer health status or political activity. Nonprofit applications often frame geofencing as a tool for efficient resource allocation and message relevance, arguing that reaching individuals at moments when they are already engaged with a cause increases the likelihood of meaningful action. These uses demonstrate that the technology is not inherently tied to foreign influence but can be adapted by any sufficiently resourced actor seeking to connect physical presence with digital persuasion.

9.3 Emerging Examples Involving Other Faith Traditions or Ideological Groups

Geofencing has also appeared in efforts targeting or originating from other faith traditions and ideological communities. Campaigns have mapped mosques, synagogues, and other religious sites in various national contexts, sometimes as part of security-related monitoring and sometimes as part of outreach or counter-messaging initiatives. Ideological gatherings, including political rallies and activist events, have similarly been enclosed by virtual boundaries to identify participants for follow-up contact or content delivery. These cases reveal that the selection of target locations often reflects the strategic priorities of the sponsoring actor rather than any fixed characteristic of the technology itself. When religious or ideological sites are chosen, the operations frequently invoke justifications of public safety, community engagement, or narrative competition. The 2025 proposal to focus on evangelical churches fits this pattern by selecting venues presumed to host audiences with particular theological or political orientations, illustrating how geofencing can be calibrated to exploit perceived correlations between physical gathering and worldview.

9.4 Lessons for Identifying and Analyzing Future Operations

Several recurring features emerge across these comparative cases that can aid in identifying and analyzing future geofencing operations. First, the technical foundation remains commercial advertising infrastructure rather than bespoke surveillance systems, which allows operations to scale rapidly once funding and intermediary relationships are in place. Second, the choice of target locations frequently reflects assumptions about the demographic or attitudinal composition of people present at those sites, whether churches, protest grounds, or medical facilities. Third, transparency mechanisms such as foreign agent registration or election disclosure laws can surface operations that might otherwise remain invisible, though they do not necessarily prevent execution or impose substantive limits on venue selection. Fourth, public and institutional reactions often intensify when sensitive locations are involved, prompting adjustments in strategy or emphasis on alternative outreach methods. Analysts seeking to recognize emerging operations can therefore focus on sudden increases in location-based advertising around particular categories of venues, disclosures under relevant regulatory frameworks, and patterns of messaging that appear contextually linked to physical presence at those sites. These indicators, combined with attention to the identity and funding of sponsoring

entities, provide a practical framework for anticipating and evaluating future applications of geofencing in both religious and non-religious domains.

10. Countermeasures, Resilience, and Policy Options

The technical capacity to geofence smartphones and deliver targeted messaging based on presence at specific locations creates corresponding needs for protective measures at multiple levels. Individuals, communities, technology platforms, and regulatory institutions each possess partial but meaningful capacity to limit unwanted capture and influence. The 2025 proposal to geofence churches and Christian colleges demonstrated both the feasibility of such operations and the value of proactive responses once plans become visible. This section outlines practical countermeasures available to individuals and communities, interventions that platforms and operating systems can implement, regulatory and legislative directions that could strengthen oversight, and the distinctive role religious institutions can play in establishing boundaries around external digital engagement.

10.1 Individual and Community-Level Technical Protections

Individuals can reduce their exposure to geofencing by managing location permissions on a per-application basis, granting access only when strictly necessary and preferring “while using the app” over “always allow.” Regularly resetting advertising identifiers in device settings disrupts the persistence of device-level tracking used for audience building and retargeting. Employing privacy-focused browsers, virtual private networks, and applications that limit background data sharing can further constrain the signals available to advertising networks. At the community level, congregations and faith-based organizations can develop shared digital hygiene practices and educational resources that inform members about how location data moves through commercial ecosystems. Awareness programs that explain the connection between physical presence at worship and potential digital targeting can empower individuals to make more deliberate choices about device configuration and app usage without requiring technical expertise from every participant.

10.2 Platform, Browser, and Operating System Interventions

Technology platforms and operating system providers control critical choke points in the data flows that enable geofencing. Enhanced permission models that make the downstream uses of location data more transparent at the moment of consent could improve user understanding. Operating systems could introduce stronger defaults that limit background location access and provide clearer signals when location data is being shared with advertising libraries. Platforms that operate real-time bidding systems for advertising could develop and enforce category-specific policies that restrict or require additional review for campaigns targeting sensitive

locations such as places of worship, medical facilities, or schools. Browser vendors can expand built-in protections against cross-site tracking that rely on location signals. While commercial incentives may limit voluntary adoption of the most restrictive measures, competitive pressure from privacy-conscious users and the threat of regulatory action can encourage incremental improvements in default settings and transparency features.

10.3 Regulatory and Legislative Proposals

Current regulatory frameworks provide partial safeguards but leave notable gaps in addressing location-based influence directed at sensitive venues. Strengthening data broker oversight, particularly regarding the sale of location data derived from religious or other protected sites, could reduce the raw material available for geofencing operations. Policymakers could consider requirements for heightened transparency or prior review when advertising campaigns target locations associated with religious exercise, political assembly, or medical care. Amendments to foreign agent disclosure statutes could require more granular reporting of targeting methodologies and venue categories, enabling earlier public scrutiny. Sector-specific rules that treat precise location data from places of worship as especially sensitive personal information would align regulatory treatment with the social and ethical weight these venues carry. Any such measures would need to balance protection against overbreadth that might unduly restrict legitimate forms of outreach or commercial activity.

10.4 Role of Religious Institutions in Setting Boundaries

Religious institutions occupy a unique position to articulate and defend norms around the use of their physical spaces in digital targeting. Congregations and denominational bodies can adopt internal policies that address external digital engagement, including guidelines for when and how outside organizations may use church properties or member data in outreach campaigns. They can also invest in digital literacy initiatives that help members understand and manage location-based tracking. By publicly articulating expectations that their gathering spaces should not be systematically converted into nodes for external influence without meaningful consultation, religious institutions can contribute to the development of broader social norms. In the aftermath of the 2025 proposal, several affected congregations began discussing these issues internally and with denominational leadership, illustrating how visibility of targeting plans can catalyze institutional responses. Over time, coordinated action by faith communities could help establish clearer expectations for technology platforms, advertisers, and foreign actors regarding the acceptable boundaries of location-based messaging in religious contexts.

11. Future Trajectories: AI, Advanced Surveillance, and Evolving Tactics

The technical and strategic foundations of smartphone geofencing are not static. Advances in artificial intelligence, the proliferation of connected devices beyond smartphones, and the refinement of influence techniques are likely to expand both the reach and the subtlety of location-based operations. The 2025 proposal to geofence churches and Christian colleges already demonstrated how commercial infrastructure could be directed toward religious communities at scale. Future developments may intensify these dynamics while also prompting more sophisticated responses from targeted populations and institutions. This section examines emerging trajectories, including the integration of artificial intelligence into location targeting, the expansion of sensing capabilities beyond smartphones, the potential for increasingly personalized narrative delivery, and the adaptive strategies that communities and regulators may develop in response.

11.1 Integration of Artificial Intelligence with Location Targeting

Artificial intelligence is increasingly embedded in advertising platforms and data aggregation systems that support geofencing. Machine learning models can analyze historical location patterns, app usage, and inferred demographic signals to predict which individuals are most likely to be present at specific venues during particular time windows. These predictions allow for more efficient allocation of advertising resources and more precise definition of target audiences. AI systems can also dynamically adjust geofence parameters in real time based on observed movement trends or emerging events. In the context of influence operations, this capability could enable campaigns to identify and reach individuals whose behavioral profiles suggest receptivity to particular messages without relying solely on static venue boundaries. The result is a shift from relatively blunt location triggers toward more adaptive and predictive forms of targeting that continuously refine their understanding of audience composition and context.

11.2 Expansion to Wearables, Vehicles, and Ambient Sensors

Smartphones are no longer the only devices capable of reporting precise location data. Wearable devices such as smartwatches and fitness trackers continuously collect location information and often share it with associated applications and advertising ecosystems. Connected vehicles transmit detailed movement data that can be linked to individual drivers or passengers through account associations. Ambient sensors embedded in smart cities, public infrastructure, and commercial spaces further extend the reach of location tracking beyond personal devices. As these systems proliferate, the surface area available for geofencing expands significantly. An individual could be identified not only by carrying a phone into a church but also by wearing a connected device, driving a networked vehicle near the site, or

triggering environmental sensors in the surrounding area. This diffusion of sensing capabilities reduces reliance on any single device category and increases the difficulty of evading location-based identification through conventional privacy practices focused on smartphones alone.

11.3 Potential for More Sophisticated Narrative Delivery and Personalization

The combination of location data with artificial intelligence enables increasingly granular personalization of messaging. Generative systems can produce variations of content tailored to inferred individual characteristics, past responses to similar messages, or real-time contextual signals. Campaigns can conduct large-scale experimentation to determine which narrative framings, visual elements, or calls to action are most effective for specific audience segments defined partly by location history. In religious or ideological contexts, this sophistication could manifest as messages that appear highly attuned to the theological or cultural language of the target community. The 2025 proposal already incorporated plans for pastoral resources and biblically framed content; future iterations could leverage AI to generate or adapt such materials at greater speed and with finer calibration to individual or congregational profiles. The boundary between helpful contextual relevance and manipulative psychological targeting becomes correspondingly harder to discern.

11.4 Anticipating Adaptive Responses by Targeted Communities

As location-based influence techniques grow more advanced, targeted communities are likely to develop correspondingly adaptive responses. Religious institutions may invest more heavily in digital literacy programs, internal data protection policies, and collective advocacy for stronger safeguards around sensitive venues. Individuals may adopt more rigorous privacy practices, including the use of multiple devices, frequent identifier resets, and selective engagement with applications that request location access. At the regulatory level, renewed attention to data broker practices and the use of location signals from protected sites could lead to new restrictions or transparency requirements. Communities may also experiment with technological countermeasures, such as coordinated efforts to obscure location signals or the development of trusted intermediary platforms that mediate external digital engagement. The interplay between advancing offensive capabilities and evolving defensive adaptations will shape the practical effectiveness of geofencing as a tool for influence in religious and other sensitive contexts over the coming years.

12. Conclusions and Recommendations

The examination of smartphone geofencing as a mechanism for targeted influence reveals a technology that originated in commercial marketing but has been readily adapted for political, advocacy, and state-sponsored purposes. The 2025 proposal to geofence Christian churches and

colleges across multiple U.S. states illustrated how commercial location-based advertising infrastructure could be directed at religious communities with significant scale and precision. This paper has traced the technical foundations of geofencing, its evolution from retail applications to influence operations, the specific details of the documented case, the legal and regulatory environment in which such operations occur, and the ethical, social, and geopolitical implications that arise when sacred spaces become nodes in digital targeting networks. The analysis demonstrates both the power of existing systems to convert physical presence into persistent digital profiles and the partial but meaningful avenues available for protection and oversight.

12.1 Synthesis of Technical, Legal, Ethical, and Social Findings

Technically, geofencing relies on the continuous location reporting capabilities of smartphones, the widespread embedding of advertising software development kits, and the real-time bidding systems that connect device identifiers to custom audiences. These same mechanisms that enable retailers to reach nearby customers also allow any sufficiently resourced actor to identify individuals at places of worship and deliver contextually linked messaging. Legally, the Foreign Agents Registration Act provided transparency in the 2025 case but did not prevent the planning of venue-specific targeting or impose substantive restrictions on the use of commercial data flows. Privacy protections remain fragmented, and current rules offer limited safeguards against the aggregation and repurposing of location signals from sensitive sites. Ethically, the practice raises concerns about autonomy, hidden persuasion, and the instrumentalization of religious gatherings. Socially, it can affect trust within faith communities, introduce external observation into spaces many regard as protected, and generate generational and institutional tensions. Geopolitically, the episode reflects broader state strategies for shaping foreign public opinion through digital means, with religious communities treated as strategic audiences. Future trajectories involving artificial intelligence and expanded sensing capabilities suggest that these dynamics are likely to intensify rather than diminish without deliberate intervention.

12.2 Recommendations for Policymakers, Platforms, and Faith Communities

Policymakers should consider strengthening oversight of location data derived from sensitive venues, including clearer rules for data brokers and requirements for heightened transparency when geofencing campaigns target places of worship, schools, or medical facilities. Enhanced reporting under foreign agent statutes could include more specific disclosure of targeting methodologies and venue categories. Technology platforms and operating system providers should improve default privacy settings, increase transparency around the downstream uses of location data, and develop enforceable policies that limit or require review for campaigns directed at sensitive locations. Faith communities can strengthen their own resilience by developing internal digital literacy resources, adopting policies regarding external digital

engagement on or near their properties, and participating in broader advocacy for protections that recognize the distinctive character of religious gathering spaces. Coordinated action across these levels offers the most promising path toward reducing the most problematic applications of geofencing while preserving space for legitimate forms of outreach and public discourse.

12.3 Areas for Further Research and Interdisciplinary Inquiry

Several areas merit sustained scholarly attention. Longitudinal studies could examine the long-term effects of location-based messaging on religious belief, community cohesion, and perceptions of institutional autonomy. Comparative research across different faith traditions and national contexts would illuminate how cultural and theological frameworks shape responses to digital targeting. Technical research into more robust privacy-preserving location technologies and detection methods for influence operations could support both individual protections and regulatory enforcement. Interdisciplinary work combining insights from computer science, religious studies, ethics, and international relations would be particularly valuable in developing nuanced frameworks for evaluating when location-based influence crosses from legitimate advocacy into forms of manipulation or undue interference. Finally, ongoing monitoring of regulatory developments and platform policies will be necessary to assess whether current gaps are being addressed or whether new forms of location-based influence are emerging faster than protective measures can adapt.

13. References

1. Show Faith by Works, LLC. Foreign Agents Registration Act Registration Statement and Exhibit AB. U.S. Department of Justice, National Security Division, FARA Registration Unit, received September 27, 2025.
2. Schnitger, Chad. Statements regarding revisions to Show Faith by Works outreach plans. Reported in Christianity Today, November 25, 2025.
3. Responsible Statecraft. “Israel wants to pay US pastors a stipend to spread the word.” October 15, 2025.
4. United Methodist News. “Firm plans to target churches with pro-Israel ads.” December 5, 2025.
5. Times of Israel. “Israel to spend up to $4.1M in bid to bolster support among Christians in western US.” October 4, 2025.
6. Jewish Telegraphic Agency. “Israel to spend up to $4.1M to bolster support among Christians in western US, filings show.” October 3, 2025.
7. Federal Trade Commission. Enforcement actions concerning data brokers and sensitive location data. Various actions, 2024–2025.
8. Electronic Privacy Information Center. Comments on geofencing and location data privacy. 2025.
9. NPR. “How Political Campaigns Are Using ‘Geofencing’ Technology To Target Catholics At Mass.” February 6, 2020.
10. Azira. “What is Geofencing Marketing and How Does it Work?” Industry analysis, 2024.
11. Adjust. “How to set up geofencing marketing.” Technical guide, 2023.
12. Radar. “What is geofencing? Geofencing definition, history, and use cases.” 2025.
13. Washington Spectator. “Israel Mounts Lavish Campaign to Win Back Evangelicals.” January 8, 2026.
14. MintPress News. Reporting on newly released FARA documents regarding Show Faith by Works. June 2026.
15. Al Jazeera. “How is Israel using US PR firms to frame its Gaza war?” October 30, 2025.
16. California Consumer Privacy Act and subsequent amendments (CPRA). California Civil Code, Division 3, Part 4.

17. U.S. Department of Justice. Foreign Agents Registration Act, 22 U.S.C. § 611 et seq.

18. Zittrain, Jonathan. *The Future of the Internet and How to Stop It*. Yale University Press, 2008 (updated editions).

19. Zuboff, Shoshana. *The Age of Surveillance Capitalism*. PublicAffairs, 2019.

20. Citron, Danielle Keats. "Sexual Privacy." *Yale Law Journal*, vol. 128, 2019.

21. Cohen, Julie E. "What Privacy Is For." *Harvard Law Review*, vol. 126, 2013.

22. Tufekci, Zeynep. "Algorithmic Harms Beyond Facebook and Google: Emergent Amplification and the Use of Algorithms in Political Advertising." *Colorado Technology Law Journal*, 2019.

23. Howard, Philip N. *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up*. Yale University Press, 2015.

24. Woolley, Samuel C., and Philip N. Howard, eds. *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford University Press, 2018.

25. Marwick, Alice E., and Rebecca Lewis. "Media Manipulation and Disinformation Online." Data & Society Research Institute, 2017.

The author has published over 5,600 AI-assisted papers at: https://www.researchgate.net/profile/Douglas-Youvan/research . Google Scholar has indexed these preprints, and if you want a particular reference, the AI mode of a Google search (Gemini) has efficiently catalogued these preprints.